

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

U.S. Department of Justice and the Federal Trade Commission

On Request for Comment Regarding Draft Merger Guidelines

FTC-2023-0043-0001

September 18, 2023

By notice published on Wednesday, July 19, 2023, the Department of Justice (DOJ) and the Federal Trade Commission (FTC) released revised draft Merger Guidelines for public comment. The draft Guidelines use modern frameworks and market realities to consolidate and replace other versions of Merger Guidelines currently in effect.¹ Within the Guidelines' catalog of analytical methods, "the Agencies assess any relevant and meaningful evidence to evaluate the effect of a merger[.]"² The Electronic Privacy Information Center (EPIC) submits these comments to encourage the DOJ and FTC to consider data protection and consolidation in merger reviews.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.³ For over two decades, EPIC has urged the FTC to assess consumer privacy impacts when reviewing proposed

¹ FTC & DOJ, *Draft Merger Guidelines*, FTC-2023-0043-001 (July 19, 2023), https://www.justice.gov/d9/2023-07/2023-draft-merger-guidelines_0.pdf [hereinafter *Draft Merger Guidelines*].

² *Id.* at 5.

³ *About Us*, EPIC (2023), <https://epic.org/about/>.

mergers between companies that engage in data collection activities.⁴ In today’s increasingly data-driven economy, mergers and acquisitions frequently involve the consolidation of commercial and proprietary data sets. Mergers implicating the consolidation of personal data can entrench a firm’s dominant market position, raise barriers to entry for new and smaller firms, and exacerbate the effects of harmful consumer data practices.

I. Merger Guidelines Should Consider Data Protection

In revising the Guidelines, the DOJ and FTC focused on three core goals, including “provid[ing] frameworks that reflect the realities of our modern economy and the best of modern economics and other analytical tools.”⁶ In 2023, the collection and monetization of personal data fuels the modern economy in a wide range of markets.⁷ Businesses’ mass accumulation of personal data produce anticompetitive effects that pose acute risks to consumer privacy, undermines data security, and subverts consumer choice. Data aggregation and consumer privacy are central to many modes of merger analysis outlined in the thirteen draft Merger Guidelines. In particular, Agencies must include data protection as a material consideration when evaluating how a merger could lessen competition (Guideline 5); entrench, or extend a dominant position (Guideline 7); impact barriers for potential entrants (Guideline 4); and impact concentration in

⁴ See Comments of EPIC, Assessment of the FTC’s Prior Actions on Merger Review and Consumer Privacy, FTC File No. P143100 at 3-20 (Mar. 17, 2015), <https://epic.org/wp-content/uploads/privacy/internet/ftc/Merger-Remedy-3-17.pdf>. See *Competition and Privacy*, EPIC (2023), <https://epic.org/issues/consumer-privacy/competition-and-privacy/>.

⁶ Press Release, Federal Trade Commission, *FTC and DOJ Seek Comment on Draft Merger Guidelines* (July 19, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-doj-seek-comment-draft-merger-guidelines>.

⁷ See, e.g., Comments of EPIC, CFPB Request for Information Regarding Data Brokers, 88 Fed. Reg. 16, 962 at 2-14 (July 14, 2023) <https://epic.org/wp-content/uploads/2023/07/EPIC-CFPB-data-brokers-RFI-comments-071423.pdf> (data lifecycle and business of data brokers).

markets (Guideline 1).⁸ Moreover, Agencies must be mindful of the ways that a business’s aggregation of and control over personal data contribute to an analysis of market definition and market power.⁹

II. Consumer Choice and Privacy in Merger Guidelines

Across the economy, data-driven competition and the “power gained by digital platforms through their control and accumulation of data” inflict anticompetitive harms.¹⁰ Mergers that involve the “control and accumulation” of data can implicate market concentration or further entrench a firm’s dominant position, reinforcing or creating barriers for potential entrants. For example, firms engaging in surveillance-based advertising and profiling have been able to entrench their dominance through their access and use of consumer data.¹¹ The broader commercial surveillance system incentivizes firms to extract large amounts of personal data to build detailed profiles, aggregate behavioral insights, or otherwise sell consumer data for targeted advertising or other purposes.¹² In a vicious cycle, “dominant firms continue to extract

⁸ See Draft Merger Guidelines, *supra* note 1 at 3-4 (Guidelines 1, 2, 4, 5, 6, 7, 8, 10).

⁹ Elettra Bietti, *Data, Context and Competition Policy*, UChicago Booth Stigler Center: Promarket (Mar. 13, 2023), <https://www.promarket.org/2023/03/31/data-context-and-competition-policy/> (“[A]gencies are recognizing that the ability to control, collect and use data contributes to a firm’s market power. Data provides market actors with knowledge about their customers, users and competitors. This knowledge can lead to unfair and exclusionary market practices.”)

¹⁰ Erika M. Douglas, *The New Antitrust/Data Privacy Interface*, 130 Yale L. J. Forum 647, 659 (Jan. 18, 2021), https://www.yalelawjournal.org/pdf/DouglasEssay_pv1pt6ak.pdf.

¹¹ Comments of EPIC, FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 22 (Nov. 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillanceANPRM-comments-Nov2022.pdf>.

¹² See *Id.*

more data and profit from trapped users, while raising barriers to entry that serve to further deprive those users of viable alternatives.”¹³

The Artificial Intelligence (AI) market—particularly generative AI—is already experiencing anticompetitive practices that entrench market power within a select few leading AI companies. Generative AI tools require a tremendous amount of money, resources, and data to develop, use, and maintain.¹⁴ The dominance of a handful of companies like OpenAI “in not only developing generative AI but also providing the underlying tools and services that generative AI requires, further concentrates a market that, despite promoting ‘open source’ technologies, is captured by a few powerful companies with opaque AI development methods[.]”¹⁵ The more data that an AI developer obtains—whether through direct web scraping, user solicitations, data broker sales, or other methods—the more powerful its AI model can be, and mergers can be one of the most efficient ways for increasing the amount of training data available to an AI firm. Similar to other online business models, generative AI services like ChatGPT and DALL-E require copious amounts of consumer data to function and compete, and consumers have little control over which companies have access to their data or how that data is used. Therefore, merger evaluations between any digital platforms or firms that amass consumer data must necessarily account for consumer privacy and security.

¹³ Accountable Tech, *Petition for Rulemaking to Prohibit Surveillance Advertising* 20 (Sept. 28, 2021), <https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf>.

¹⁴ EPIC, *Generating Harms: Generative AI’s Impact & Paths Forward* 57 (May 2023), <https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf> (“To maintain the underlying computing power necessary to run ChatGPT, for example, experts have estimated that OpenAI must spend roughly \$700,000 a day, 180 leading to an estimated \$540 million loss for OpenAI in 2022 alone.”).

¹⁵ *Id.* at 58.

Competition drives innovative privacy policies and protections that benefit consumers, whereas “recent characterizations of digital market power and abuse of dominance . . . link the decline of competition with the erosion of data privacy.”¹⁶ In the context of mergers, consolidation can threaten consumer privacy when companies that protect user privacy absorb companies that fail to protect privacy.¹⁷ As we have previously warned, “If the largest internet firms continue to buy up new market entrants and assimilate their users’ data into the existing platforms then there will be no meaningful opportunity for firm to compete with better privacy and data security practices.”¹⁸

III. Conclusion

A competitive market benefits consumer data privacy and security by incentivizing strong privacy and data security policies and enabling consumer choice. As consumer data continues to fuel our data-driven economy, it is critical that the Draft Merger Guidelines include privacy considerations to ensure that both competition and consumers are protected in merger reviews. If you have any additional questions, please contact EPIC Law Fellow Suzanne Bernstein at bernstein@epic.org.

Sincerely,

/s/ John Davisson
EPIC Director of Litigation
& Senior Counsel

¹⁶ Douglas, *supra* note 10 at 656.

¹⁷ EPIC, Statement to Senate Judiciary Committee, Hearing on Antitrust Enforcement Oversight 3 (Oct. 3, 2018), <https://archive.epic.org/testimony/congress/EPIC-SJC-AntitrustOversight-Oct2018.pdf>.

¹⁸ EPIC, Statement to House Judiciary Committee Regarding Online Platforms and Market Power, 4 (July 28, 2020), <https://epic.org/documents/online-platforms-and-market-power-part-6-examining-the-dominance-of-amazon-apple-facebook-and-google/>.

/s/ Suzanne Bernstein
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)